UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

Crim. No. 07-226 (WJM)

v.

OPINION

GEORGE PAYNE

HON. WILLIAM J. MARTINI

For the United States:

Dustin Chao
Assistant United States Attorney
Marc Larkins
Assistant United States Attorney
United States Attorney's Office
970 Broad Street
Newark, NJ 07102

For the Defendant:

Denis Kelleher Kelleher & Dunne LLP 17 Battery Place, 11th Floor New York, NY 10004

MARTINI, U.S.D.J.:

This matter comes before the Court on the Superseding Indictment of Defendant George Payne, who was charged with (1) receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), and (2) possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

Defendant waived his right to a trial by jury on August 24, 2007. On

September 5, 2007, this Court presided over a bench trial at which the parties jointly submitted six stipulations in lieu of testimony. The Government admitted a series of exhibits into evidence with no objection.

FINDINGS OF FACT

Based on all of the evidence in the record, including the stipulations of the parties concerning the testimony of witnesses Special Agent Howard M. Martinez, Detective Denny H. Wood, Special Agent Victoria Becchina, Senior Special Agent Christopher J. Doyle, and Richard Boland, a custodian of records for Citibank, and the exhibits admitted into evidence, this Court makes the following findings of fact:

A. The Investigation

- 1. In May 2005, agents at Immigration and Customs Enforcement (ICE) were investigating an individual in Monmouth County, New Jersey, not Defendant George Payne, and recovered child pornography on that individual's computer. During that investigation, the agents came across suspicious e-mails from the e-mail address theodore_dykstra@hotmail.com (the "Dykstra account"). (Stip. 4, ¶ 5.)
- 2. While searching this computer, agents discovered an e-mail with references to child pornography that directed the recipient to go to the web address of http://orbita.starmedia.com/kdaharda/1/main.html. Using terms like

- "orbita" and "starmedia," agents were eventually led to a website that labeled itself "Illegal.CP." (Stip. 4, ¶¶ 6-8.)
- 3. ICE agents then discovered that the Illegal.CP website had three banner pages: (a) Illegal.CP, (b) Children Porno, and (c) The Sick Child Room. (See Exhs. A1, A2, and A3.) Each of the three banner pages had graphic images of prepubescent children engaged in sexually explicit acts, along with testimonials or language advertising the child pornography contained on the website. (See id.) All three banner pages contained links that led to a "Join page," where a user was asked to input his personal and financial identification information to gain a subscription to Illegal.CP. (Stip. 4, ¶ 8, Exh. A4.)

B. The Undercover Subscription

- 4. On October 26, 2005, ICE agents accessed the "Join page" and entered credit card information to gain an undercover subscription to the Illegal.CP website. The undercover application was approved the next day via an email sent to the undercover from the Dykstra account. This next day notification was promised on the Illegal.CP "FAQ" page that greeted the user every time a user logged onto the Illegal.CP site. (Stip. 4, ¶¶ 9-10, Exhs. A5, A8.)
- 5. With this subscription in hand, ICE agents tracked the IP address of the

Illegal.CP site from October through November of 2005, and discovered that the Illegal.CP site (along with its thousands of images of child pornography) was being housed on a web server in Orlando, Florida by a company called HostDime.com. Agents also discovered that there were hundreds of subscribers who were accessing the Illegal.CP site during their surveillance of the site. (Stip. 4, ¶ 13.)

- 6. After executing three search warrants on the HostDime.com server from November to December 2005, and initiating an e-mail intercept in late December of 2005, ICE agents learned that the web server housing the Illegal.CP website had moved to another web server in McLean, Virginia owned by a company called HopOne. (Stip. 4, ¶¶ 13-16.)
- 7. After locating the HopOne server, ICE executed a search warrant on February 1, 2006 for the contents of Illegal.CP as housed on the HopOne server. This search warrant revealed thousands of images and videos of child pornography contained on the Illegal.CP website, which were then copied to Government Exhibit A11 for the purpose of this trial. A final search warrant on the HopOne server showed that the Illegal.CP website shut down for a few days after February 7, 2006, and then was reestablished at a new IP address (85.249.22.169) on a web server located in Russia. (Stip. 4, ¶ 16.)

C. The Dykstra Account E-mail Intercepts

- 8. After receiving the October 27, 2005 e-mail from the Dykstra account approving its undercover subscription, ICE obtained court approval to intercept the e-mail traffic to and from the Dykstra account in order to learn more about the account itself and to locate other potential subscribers to the Illegal.CP site. (Stip. 4, ¶ 14.)
- 9. With court approval to intercept e-mail traffic to and from the Dykstra account from December 27, 2005 to January 25, 2006, and from January 27, 2006 to February 25, 2006, ICE was able to observe the mechanics of the subscription and approval process through the Dykstra account. Through these intercepts, ICE learned that credit card information was verified through communications among the Dykstra account and individuals operating the e-mail addresses joe777@mail.ru and admin@sib-games.com. (Stip. 4, ¶ 14.)
- 10. In addition to personal identification and credit card information being transmitted between the Dykstra account and the joe777@mail.ru account, other information relating to prospective subscribers was also captured in these communications. This information, which amounted to a detailed business receipt of the transaction, included the IP address of the subscriber and information as to which Banner Page the user entered prior to inputting

his information on the "Join page." After subscribers were approved via these e-mail communications, the Dykstra account would then send an e-mail to the user to notify him that his subscription was approved. ICE observed hundreds of individuals getting approved for membership to the Illegal.CP site during the two-month period of the intercepted communications. (Stip. 4, ¶¶ 14, 15, 17, Exh. A6.)

D. Locating Defendant George Payne through the Dykstra Account Intercept

- 11. Through the Dykstra account intercepts, ICE agents located George Payne as an approved subscriber to the Illegal.CP website. In an e-mail from the Dykstra account to joe777@mail.ru, dated February 11, 2006, George Payne's name, credit card, address, his personally chosen login and password, as well as his IP address, and the information as to the Banner Page he entered prior to subscribing were all contained therein. (Stip. 4, ¶ 17, Exh. A6.)
- 12. The Dykstra account intercept also revealed the Dykstra account e-mail that was sent the next day, February 12, 2006, to gpayne999@yahoo.com approving the subscription to Illegal.CP. (Stip. 4, ¶ 19, Exh. A6-c.)
- 13. In fact, a simple comparison of the Dykstra account e-mail sent to Payne on

February 12, 2006 to the Dykstra account e-mail sent to ICE's undercover account on October 27, 2005 provides powerful corroboration that the Defendant was approved for a paid subscription to the Illegal.CP website. For example, both Dykstra e-mails: (a) greeted the recipient with the login and password of his own choosing; (b) notified the recipient that he was billed \$79.99 to AD SOFT for a 20-day membership; (c) had Internet links to three sites (all with spaces in between the letters to avoid spam blockers) that each led to Illegal.CP; (d) contained the same Internet link "pliac.hotfire.net," which led to the Illegal.CP website; and (e) contained a note admonishing the recipient to respond to other people asking about the charge to AD SOFT by lying that it constitutes a purchase of spyware software. (Exhs. A5, A6-c.)

14. More importantly, however, was the corroboration provided by the February 11, 2006 e-mail from the Dykstra account to joe777@mail.ru, referenced in paragraph 11 above. In other words, while the February 12, 2006 Dykstra e-mail to gpayne999@yahoo.com confirmed that the Defendant received a subscription to Illegal.CP (indeed, this e-mail was recovered on the Defendant's own Fireball hard drive, *see* Stip. 5, ¶¶ 15-16, Exhs. E4-E5), the Dykstra e-mail to joe777@mail.ru not only confirmed that the

Defendant visited the Illegal.CP site from his home computer (from IP address 67.85.0.77), but also confirmed the actual Banner Page that the Defendant had viewed prior to submitting his application to Illegal.CP, *i.e.*, The Sick Child Room. Moreover, the Sick Child Room Banner Page, with URL address beginning fidurozagucai.net, was captured by ICE agents, and is contained in Government Exhibit A3 representing the way it appeared on February 10, 2006, the day before the Defendant's Citibank credit card was charged \$79.99 to AD SOFT. (Stip. 4, ¶¶ 8, 17, 19, Exhs. A3, A6; Stip. 5, ¶¶ 14-15, Exhs. E3-E4.)

E. The Defendant's Yahoo! Account and Internet Service Provider Records

- 15. After reviewing the Dykstra intercepts to gpayne999@yahoo.com, ICE continued its investigation as to the Defendant by requesting business records from Citibank, Yahoo!, and Optimum Online. (Stip. 4, ¶¶ 20-22, Exhs. C1-C3, B1-B2.)
- 16. The Yahoo! records pertaining to gpayne999@yahoo.com showed that this e-mail account belonged to George Payne, that the account was active, and that on February 12, 2006, someone had logged onto the gpayne999@yahoo.com account from IP address 67.85.0.77, the

- Defendant's home computer IP address. (Stip. 4, ¶ 21, Exh. B1.)
- 17. The Optimum Online records pertaining to IP address 67.85.0.77 showed that the account belonged to George Payne of 518 Monroe Street, Apt. 4A, Hoboken, New Jersey; that the e-mail accounts associated with this account were "payne999@optonline.net" and "lostsoul20@optonline.net"; and that the user had connected to the Internet via the IP address 67.85.0.77 on February 12, 2006, the day the Defendant received his subscription e-mail from the Dykstra account. (Stip. 4, ¶ 22, Exh. B2.)
- 18. Finally, ICE received the Citibank credit cards for account number 5424

 1806 8688 3478, the credit card account number listed in Government

 Exhibit A6, pertaining to the Defendant's subscription information

 transmitted on February 11, 2006 between the Dykstra account and

 joe777@mail.ru. These records revealed that this Citibank credit card

 account belonged to George Payne of 518 Monroe Street, Apt. 4A,

 Hoboken, New Jersey, with e-mail address gpayne999@yahoo.com, that

 George Payne was the primary applicant, and that George Payne was the

 sole account holder listed on the Citibank account. (Stip. 4, ¶ 20, Exhs. C1-C2.)
- 19. In addition, a review of the George Payne Citibank credit card account

showed one charge to AD SOFT for \$79.99 on February 11, 2006, and another charge to AD SOFT for \$79.99 on March 25, 2006. Although the Citibank credit card was reported stolen on March 5, 2006, neither AD SOFT charge was contested, and both charges were paid. (Stip. 6, ¶¶ 3-6.)

F. The Search Warrant at Defendant Payne's Residence

- 20. After gathering all the above information, on May 4, 2006, ICE agents, including Senior Special Agent Christopher Doyle, went to 518 Monroe Street, Apt. 4A, Hoboken, New Jersey where they found the Defendant and his companion, Elise Falanga. (Stip. 5, ¶ 3.)
- 21. At the apartment, Agent Doyle went to a separate room and recovered the hard drives from two computers. One hard drive (Fireball model hard drive) was located inside a computer unit (underneath a desk), which was connected to a monitor and keyboard. The other hard drive (Deskstar model hard drive) was near a closet in the same room. (Stip. 5, ¶¶ 3-5, Exhs. D1-D6, D11-16.)
- 22. Using specialized computer forensic software to facilitate the preservation and examination of evidence on the two hard drives recovered from the Defendant's apartment, Agent Doyle made an exact duplicate, or forensic image, of all the files contained on each of the Fireball hard drive and the

- Deskstar hard drive. (Stip. 5, ¶¶ 6-7.)
- 23. After examining the forensic images of the Fireball and Deskstar hard drives, Agent Doyle located 476 images of child pornography on the Fireball hard drive and 79 images of child pornography on the Deskstar hard drive. After comparing these 555 images to the images of child pornography from the Illegal.CP HopOne web server (Exh. A11), Agent Doyle found that on the Fireball hard drive, 76 images matched images from the Illegal.CP HopOne server, and that on the Deskstar hard drive, one image matched an image from the Illegal.CP HopOne server. (Stip. 5, ¶¶ 7-11, Exhs. A11, F1-a, F1-b, F2-F4.)

G. The Defendant's Internet Searches for Child Pornography

- 24. During Agent Doyle's forensic examination of the contents of the Fireball and Deskstar hard drives, he found web pages on the Deskstar relating to 20 searches, dating from 2002 to 2005, that were performed on Google using terms like "childlover," "pre-teen sex," "nymphets," "lolita," and "young child sex stories." On the Fireball, Agent Doyle found 20 Internet Explorer searches, dated from 2005 to 2006, using terms like "father daughter incest" and "father son incest." (Stip. 5, ¶¶ 12-13, Exhs. E1-E2.)
- 25. Agent Doyle found five e-mails from the Defendant's

gpayne999@yahoo.com account (two on the Fireball, and three on the Deskstar), dated from March 2005 to April 2006, containing advertisements for child pornography websites. In addition, Agent Doyle found several files containing the terms "lostsoul20" and "14lost" on each hard drive, including a file on the Deskstar which showed that "14lost" was chosen as a password for an account with Staples.com. Included among these files was the February 12, 2006 e-mail sent from the Dykstra account to the Defendant's gpayne999@yahoo.com account, approving the Defendant's subscription to Illegal.CP. (Stip. 5, ¶¶ 14-16, Exhs. E3-E5.)

26. Finally, perhaps the most powerful evidence showing that the Defendant (i) sought Illegal.CP, (ii) found Illegal.CP, and (iii) accessed the pictures on Illegal.CP, is contained in Government Exhibit E1, page 23 — where "orbita.starmedia.com" appeared in a Google search performed on the Defendant's Deskstar hard drive — and Government Exhibit E2, page 1 — where the terms "lostsoul20" and "14lost" were input on Defendant's Fireball hard drive on March 17, 2006 and March 18, 2006 on a website with an IP address of 85.249.22.169, the last known IP address of Illegal.CP (in Russia). (Stip. 5, ¶ 13, Exh. E12.)

H. The Images on the Defendant's Computer were Child Pornography

- 27. At least three images found on the Defendant's Fireball and Deskstar hard drives consisted of child pornography as defined by 18 U.S.C. § 2256(8)(A). In addition, the evidence established that the Defendant received at least five images of child pornography from the Illegal.CP website. Specifically, Agent Howard M. Martinez identified two boys who were sexually molested by their mother and photographed during such episodes by their stepfather in Utah in 2003. When they were photographed, the boys were three years old and seven years old, respectively. Three images of these boys were found on the Defendant's Fireball hard drive. These images also matched images on the Illegal.CP HopOne server. (Stip. 1, ¶¶ 1-4, Exh. F1-a; Stip. 5, ¶ 9, Exh. A11.)
- 28. In addition, Detective Denny H. Wood identified two girls who were sexually molested and photographed in sexually explicit positions by their stepfather in Washington State from 2000 to 2001. When they were photographed, the girls were seven years old and nine years old,

Upon review of these three images, the Court is satisfied that the acts depicted therein constitute sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A), and that the images depict child pornography as defined in 18 U.S.C. § 2256(8)(A).

respectively. Two images of these girls were found on the Defendant's Fireball hard drive.² These images also matched images on the Illegal.CP HopOne server. (Stip. 1, ¶¶ 1-4, Exh. F1-a; Stip. 5, ¶ 9, Exh. A11.)

CONCLUSIONS OF LAW

Receipt of Child Pornography

For the offense of receipt of child pornography, the essential elements, each
of which the Government must prove beyond a reasonable doubt, are:

<u>First</u>: that the Defendant knowingly received any material that contains
child pornography;

Second: that such material containing child pornography had been transported, shipped, or mailed, in interstate or foreign commerce, by any means, including by computer, as charged; and

<u>Third</u>: that, at the time of such reception, the Defendant believed that such material constituted or contained child pornography.

2. The evidence proves beyond a reasonable doubt that the Defendant knowingly received at least three images containing child pornography.

Upon review of these two images, the Court is satisfied that the acts depicted therein constitute sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A), and that the images depict child pornography as defined in 18 U.S.C. § 2256(8)(A).

- First and foremost, the evidence establishes that the Defendant ordered two subscriptions to the Illegal.CP website, which he paid for with his own credit card. (Stip. 4, ¶ 19, Exh. A6-c; Stip. 6, ¶¶ 3-6, Exh. C1.)
- Second, the evidence shows that on or about February 11, 2006, the
 Defendant went through a banner page (the Sick Child Room) on the
 Internet which featured graphic images advertising child pornography.
 (Stip. 4, ¶¶ 8, 17, 19, Exhs. A3, A6.)
- Third, on February 12, 2006, the Defendant received the Dykstra account e-mail to his gpayne999@yahoo.com on his Fireball hard drive, which approved his membership and provided three known links to the Illegal.CP website. (Stip. 4, ¶ 19, Exh. A6-c; Stip. 5, ¶¶ 14-15, Exhs., E3- E4.)
- Fourth, 76 images on the Defendant's Fireball hard drive matched child pornography images located on the Illegal.CP HopOne web server.
 (Stip. 5, ¶¶ 7-11, Exh. A11, F1-a.)
- And fifth, the evidence has proven beyond a reasonable doubt that the Defendant possessed and controlled the Fireball and Deskstar hard drives (both computers were located at his apartment; both hard drives contained e-mails to his gpayne999@yahoo.com e-mail account; and

both hard drives contained highly personal logins (lostsoul20) and passwords (14lost) that the Defendant chose for a Staples.com account and his own Optonline.net e-mail addresses). (Stip. 5, ¶¶ 3-5, 15-16, Exhs. D1-D6; E4-E5.)

See United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998) (sufficient proof where government presented evidence that defendant's computer contained two child pornography files, the names of which were substantially similar to the names of files downloaded by him over the Internet).

- 3. The government has also proven beyond a reasonable doubt that the images containing child pornography traveled in interstate commerce.³
 - First, the Illegal.CP site served its subscribers via the Internet from servers located first in Orlando, Florida, then McLean, Virginia, and ultimately, Russia. (Stip. 4, ¶¶ 13-16.)
 - Second, Illegal.CP advertised via banner pages transmitted over the Internet, and subscriptions to Illegal.CP had to be accessed via the Internet. (Stip. 4, ¶¶ 8-10.)

The legal analysis pertaining to the interstate commerce element also further supports the Court's finding, with respect to the first element, that the Defendant knowingly received images of child pornography.

- Third, the evidence has shown that the Defendant had access to the Internet through his Optimum Online account, which provided the Defendant access to the Internet via his IP address, 67.85.0.77. (Stip. 4, ¶ 22.)
- Fourth, Yahoo! business records have shown that the Defendant was actively using his Yahoo! e-mail account of gpayne999@yahoo.com, and that on February 12, 2006, the Defendant logged on to the Internet via his Optimum Online IP address of 67.85.0.77 and accessed his Yahoo! e-mail account. (Stip. 4, ¶ 21.)
- Fifth, the Defendant's computer registry file on the Fireball hard drive showed that the Defendant had visited IP address 85.249.22.169, Illegal.CP's Russia web server location, and that the Defendant entered his login, "lostsoul20" and his password, "14lost" in March 2006 at that IP address. (Stip. 5, ¶ 13, Exh. E2.)
- And sixth, Stipulations 1 and 2 establish that three images of child pornography found on the Defendant's Fireball hard drive were produced in Utah, and two images of child pornography found on the Defendant's Fireball hard drive were produced in Washington State.

 (Stips. 1 & 2; Stip. 5, ¶ 9.)

- See United States v. MacEwan, 445 F.3d 237, 244-46 (3d Cir. 2006) (images traveling via the Internet have traveled in interstate commerce).
- 4. The evidence also proves beyond a reasonable doubt that at the time he received the images, the Defendant believed that they contained child pornography.
 - First, the evidence shows that the Defendant believed that he was receiving child pornography because he was actively looking for it. The numerous Google and Internet Explorer searches on his computers, using terms associated with child pornography, showed that the Defendant intentionally sought child pornography on the Internet. (Stip. 5, ¶¶ 12-13.)
 - Second, the e-mail communication between the Dykstra account and joe777@mail.ru concerning the Defendant's subscription shows that the Defendant entered his Illegal.CP application after clicking on the Sick Child Room banner page. (Stip. 4, ¶¶ 8, 17.)
 - Third, the Defendant paid \$79.99 for his subscription to Illegal.CP on two separate occasions February 11, 2006 and March 25, 2006.
 (Stip. 6, ¶¶ 1-6.)

See United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998) (evidence that

the defendant possessed additional child pornography could be used to show the defendant's intent and absence of mistake); *United States v. Caldwell*, 181 F.3d 104 (6th Cir. 1999) (unpublished) (a defendant's possession of child-oriented erotica was properly used to show knowledge and intent to possess child pornography).

Possession of Child Pornography

5. Similarly, for the offense of possession of child pornography, the essential elements, each of which the Government must prove beyond a reasonable doubt, are:

<u>First</u>: that the Defendant knowingly possessed any material that contains child pornography;

Second: that such material containing child pornography had been transported, shipped, or mailed, in interstate or foreign commerce, by any means, including by computer, as charged; and

<u>Third</u>: that, at the time of such possession, the Defendant believed that such material constituted or contained child pornography.

6. The evidence has proven that the Defendant knowingly possessed child pornography. In addition to the above evidence proving the Defendant's knowing receipt of child pornography, the evidence has shown that at least

three images of child pornography were found on the Defendant's hard drives. Moreover, child pornography was located on two of the computers found in Defendant's home. Furthermore, the evidence has shown that the Defendant conducted Internet searches for child pornography, that e-mails were sent to his Yahoo! account advertising child pornography, and that he paid for two subscriptions to a website dedicated to child pornography. This evidence proves beyond a reasonable doubt that the Defendant knew that he possessed images of child pornography. (Stip. 5, ¶¶ 7-13.) *See United States v. Nanda*, 178 F. 3d 1287 (4th Cir. 1999) (unpublished) (additional images of child pornography and chat-room dialogues pertaining to the same were relevant to show the defendant's knowing possession of child pornography).

- 7. The evidence proves beyond a reasonable doubt that the images of child pornography possessed by the Defendant traveled in interstate commerce. (See Receipt of Child Pornography, supra, ¶ 3.)
- 8. The evidence also proves beyond a reasonable doubt that at the time he possessed the images, the Defendant believed that they contained child pornography. (See Receipt of Child Pornography, supra, ¶ 4.)
- 9. Child pornography means "any visual depiction . . . of sexually explicit

- conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct" 18 U.S.C. § 2256(8)(A).
- 10. "Visual depiction" includes any undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 U.S.C. § 2256(5).
- 11. "Sexually explicit conduct" means actual or simulated (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (B) bestiality; (C) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person. 18 U.S.C. § 2256(2).
- 12. The term "minor" means any person under the age of eighteen years. The term "minor" includes only natural persons, and does not include images that were produced without using a real person, for example, through the use of digital or virtual creations of an image that appears to be a minor. For the purpose of the statute, under the age of eighteen refers to the person's age at the time when the visual depiction of that person engaging in sexually explicit conduct was produced. 18 U.S.C. § 2256(1); *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

- 13. The government has proven beyond a reasonable doubt that at least three of the 555 images contained in Government Exhibits F1-a, F1-b, F2, and F3 meet the definition of child pornography in 18 U.S.C § 2256(8)(A).
- 14. The Government has proven beyond a reasonable doubt that the Defendant knew that at least three of the images he possessed depicted real, minor children. The Illegal.CP website, itself, advertised its use of actual children in selling images to subscribers such as the Defendant. The images speak for themselves. No reasonable person could not know that these images showed minors engaged in sexually explicit conduct. The only conclusion acceptable based upon the evidence is that a reasonable person would believe that the images are exactly what they appear to be real children.
- 15. The Government has proven beyond a reasonable doubt that the Defendant knew the general nature, character and content of the images. Once again, the images speak for themselves; no reasonable person viewing these images could deny that they are exactly what the United States proved them to be. The Defendant purposefully sought these images out, performing Internet searches in his quest for child pornography, and purchased them with his credit card over the Internet from a website that advertised itself as providing "illegal" images of children. *See United States v. Titchell*, 261

- F.3d 348, 351 (3d Cir. 2001); *United States v. Wert-Ruiz*, 228 F.3d 250, 254-55 (3d Cir. 2000); *United States v. Stewart*, 185 F.3d 112, 126 (3d Cir. 1999); *United States v. Caminos*, 770 F.2d 361, 366 (3d Cir. 1985).
- 16. Finally, the government has proven beyond a reasonable doubt that the child pornography Defendant possessed was transported in interstate commerce and that the child pornography was produced using materials that had been mailed or shipped or transported in interstate or foreign commerce by any means, including a computer. The Defendant sought and received his subscription to Illegal.CP through his Yahoo! e-mail account, and in addition to the overwhelming evidence that Defendant used the Internet to receive child pornography, forensic examinations provided proof that he used his computer to visit the Illegal.CP site when the web server was located in Russia. *See United States v. MacEwan*, 445 F.3d 237, 244-46 (3d Cir. 2006).

Based on the foregoing, the Court concludes that the Government has proven each element of both offenses beyond a reasonable doubt. Therefore, the Court finds the Defendant, George Payne, guilty of (1) receiving child pornography, in violation of 18 U.S.C. §2252A(a)(2)(A), and (2) possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

MOTION FOR MODIFICATION OF BAIL CONDITIONS

Defendant also filed a pre-trial motion seeking an order modifying his bail conditions to remove home detention and electronic monitoring, which this Court imposed after the Government added a charge of receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) by way of the Superseding Indictment.

The Bail Reform Act, as amended by the Adam Walsh Child Protection and Safety Act of 2006, specifies that in any case involving a minor victim under § 2252A(a)(2)(A) (among other sections), "any release order shall contain, at a minimum, a condition of electronic monitoring" and five other conditions. *See* 18 U.S.C. § 3142(c)(1)(B). Defendant argued that the amended Bail Reform Act is unconstitutional because it mandates these special release conditions in every case, without discretion, based solely on the offense charged.

At oral argument on August 20, 2007, the Court reserved judgment on this issue, which raises a novel argument not yet addressed by many courts. Because this Court now finds Defendant found guilty beyond a reasonable doubt, however, Defendant is no longer subject to conditions of pre-trial detention, and Defendant's Motion for Modification of Bail Conditions is moot. Therefore, Defendant's motion is denied.

CONCLUSION

An appropriate Order accompanies this Opinion.

Dated: October 25, 2007

s/William J. Martini
William J. Martini, U.S.D.J.